BOARD OVERSIGHT OF MANAGEMENT’S RISK APPETITE & TOLERANCE: THE NEW GLOBAL IMPERATIVE

TIM LEECH, FCPA, CIA, CRMA, CCSA, CFE
MANAGING DIRECTOR GLOBAL SERVICES
RISK OVERSIGHT INC.
SPONSORED BY: BPS RESOLVER

March 27, 2013
Your Presenter

Tim Leech
Managing Director Global Services
Risk Oversight Inc.
www.riskoversight.ca
tim.leech@riskoversight.ca
About Your Presenter

Tim J. Leech, FCPA CIA CRMA CCSA CFE is Managing Director Global Services at Risk Oversight Inc. (“RO”) He has over 30 years of experience in the ERM, internal audit, IT, and forensic accounting fields. His experience base includes setting up a new business unit for Coopers & Lybrand, Control & Risk Management Services, in 1987; founding, building, and successfully selling CARD®decisions, a global risk and assurance consulting and software firm, to Paisley/Thomson Reuters from 1991 to 2004; serving as Paisley’s Chief Methodology Officer from 2004 -2007; and global experience helping clients with internal audit transformation initiatives and the design, implementation, and maintenance of integrated GRC/ERM methodology and technology frameworks. He developed and successfully released CARD®map, the world’s first integrated risk and assurance software, in 1997. The web-enabled “cloud” version of CARD®map was released in 2000. He has delivered IIA IPPF Standard 2120 training on how to assess and report on the effectiveness of risk management processes to internal auditors and risk specialists in locations around the world. He is the author of the December 2012 Conference Board Director Notes publication “Board Oversight of Management’s Risk Appetite and Tolerance” and the globally acknowledged RO white paper “The High Cost of ERM Herd Mentality”. Risk Oversight Inc. and BPS Resolver will be launching RiskStatusNet™ - “next generation” ERM/GRC software in mid 2013. In 1997 Leech was awarded the designation Fellow of the Ontario Institute of Chartered Accountants (FCPA/FCA) in recognition of his public service and contributions in the fields of risk and control management. In September 2009 Tim was awarded the first ever IIA Canada Outstanding Contributor to the Profession of Internal Auditing award in recognition of over 25 years of global service to the internal audit profession.
Agenda

• Evolution of risk oversight expectations
• ERM scorecard to date
• Traditional “Supply Driven” IA & ERM - What’s wrong with the status quo?
• Why Change your IA/ERM approach?
• Board Driven/Objective-centric (“BD/OC”) IA & ERM
• BD/OC IA & ERM – Step by Step
• Business case for BD/OC IA & ERM
• BD/OC - Next Generation Risk & Assurance Technology
• Questions
Evolution of Risk Oversight Expectations

Bear Stearns bailout

J.P. Morgan and N.Y. Fed provide funds to strapped Wall St. broker

So long, Bear Stearns BSC

Final bid, $2

Lehman collapse sends shockwave round world

AIG Faces $17B in Collateral Calls

FannieMae

Freddie Mac

Bloomberg
Evolution of Risk Oversight Expectations
Evolution of Risk Oversight Expectations

Senior Supervisors Group issued three important reports:

3. December 23, 2010 “Observations on Developments in Risk Appetite Frameworks and IT Infrastructure”

Evolution of Risk Oversight Expectations

NACD Board Risk Oversight Criteria

While risk oversight objectives may vary from company to company, every board should be certain that:

- the risk appetite implicit in the company’s business model, strategy, and execution is appropriate.
- the expected risks are commensurate with the expected rewards.
- management has implemented a system to manage, monitor, and mitigate risk, and that system is appropriate given the company’s business model and strategy.
Evolution of Risk Oversight Expectations

While risk oversight objectives may vary from company to company, every board should be certain that:

• The risk management system informs the board of the major risks facing the company.
• An appropriate culture of risk-awareness exists throughout the organization.
• There is recognition that management of risk is essential to the successful execution of the company’s strategy.

Evolution of Risk Oversight Expectations

A FRAMEWORK FOR BOARD OVERSIGHT OF ENTERPRISE RISK

by John E. Caldwell, CA

INSTITUTE OF CORPORATE DIRECTORS
Evolution of Risk Oversight Expectations

• IIA’s IPPF 2120 Risk Management Standard effective 2010 states internal auditors “must” evaluate the effectiveness and contribute to the improvement of risk management processes.

Evolution of Risk Oversight Expectations

Per IIA IPPF 2120:
Determining whether risk management processes are effective is a judgment resulting from the internal auditor’s assessment that:

• Organizational objectives support and align with the organization’s mission;
• Significant risks are identified and assessed;
• Appropriate risk responses are selected that align with the organization’s risk appetite; and
• Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Evolution of Risk Oversight Expectations

CSA Expectations: Canadian Public Companies

Material risks are required to be disclosed in regulatory filings such as an AIF or a prospectus. The way in which an issuer manages those risks may vary between industries and even between issuers within an industry according to their particular circumstances. It is important for investors to understand how issuers manage those risks.

Disclosure regarding oversight and management of risks should indicate:

• the board’s responsibility for oversight and management of risks, and
• any board and management-level committee to which responsibility for oversight and management of risks has been delegated.

The disclosure should provide insight into:

• the development and periodic review of the issuer’s risk profile
• the integration of risk oversight and management into the issuer’s strategic plan
• the identification of significant elements of risk management, including policies and procedures to manage risk, and
• the board’s assessment of the effectiveness of risk management policies and procedures, where applicable.

(Source: CSA STAFF NOTICE 58-306 2010 CORPORATE GOVERNANCE DISCLOSURE COMPLIANCE REVIEW
Evolution of Risk Oversight Expectations

In the U.S. it isn’t very clear yet what the SEC wants. It’s subject to “best guess” interpretation. Some “best guesses” from informed sources:


PwC has published a summary of opportunities to enhance risk-oversight practices in “Point of View” May 2010. Key conclusions – there should be no ambiguity about the board’s responsibility and “the most informative disclosures shed light on relationships and processes”. ([http://pwc.to/iNBhuJ](http://pwc.to/iNBhuJ))
Evolution of Risk Oversight Expectations

FROM THE SEC February 20, 2013:

Item 407(h) also requires companies to describe the role of the board of directors in the oversight of risk. Recently, the U.S. Government Accountability Office found that economic output losses from the 2007-2009 financial crisis could exceed $13 trillion. Given the magnitude of that crisis, which continues to be felt, it would be difficult to overemphasize the importance that investors place on questions of risk management. Has the board set limits on the amounts and types of risk that the company may incur? How often does the board review the company’s risk management policies? Do risk managers have direct access to the board? What specific skills or experience in managing risk do board members have? Issuers that offer boilerplate in lieu of a thoughtful analysis of questions such as these have not fully complied with our proxy rules and are missing an important opportunity to engage with investors.

Polling Question #1

1. Which of the following was **not** identified by commissions as one of the root causes of the 2008 global financial crisis:
   a) Deficient board oversight of risk
   b) Deficient board oversight of risk appetite/tolerance
   c) Deficient internal audit capability and processes
   d) Misaligned reward systems
   e) Don’t know

ERM SCORECARD
ERM Scorecard to Date Helping Boards Oversee Management’s Risk Appetite

The truth is that a large % of ERM initiatives have failed badly or sub-optimized.

Few meet board risk oversight criteria established by the NACD Blue Ribbon Commission “Risk Governance: Balancing Risk and Reward”
ERM Scorecard to Date Helping Boards Oversee Management’s Risk Appetite

2008 Global Financial Crisis –

Weak risk management and oversight identified as a root cause of the crisis. But most organizations at the center of the crisis had some form of ERM, and virtually all had large internal audit functions. Senior Supervisors Group study identified the following root causes in failed institutions:

• The failure of some boards of directors and senior managers to establish, measure, and adhere to a level of risk acceptable to the firm
• Compensation programs that conflicted with the control objectives of the firm
• Inadequate and often fragmented technological infrastructures that hindered effective risk identification and measurement
• Institutional arrangements that conferred status and influence on risk takers at the expense of independent risk managers and control personnel

ERM Scorecard to Date Helping Boards Oversee Management’s Risk Appetite

Limited True Adoption of ERM

Current Stage of ERM

- **36%**: Systematic, robust and repeatable process with regular reporting of aggregate top risk exposures to board.
- **28.2%**: Mostly informal and unstructured, with ad hoc reporting of aggregate top risk exposures to the board.
- **23.3%**: Mostly track risks by individual silos of risk, with minimal reporting of aggregate top risk exposures to the board.
- **12.5%**: There is no structured process for identifying and reporting top risk exposures to the board.

ERM Scorecard to Date Helping Boards Oversee Management’s Risk Appetite

COSO 2010 study disclosed that a large % of ERM initiatives were not delivering to a “significant or a great deal” key benefits promised by ERM promoters

ERM Scorecard to Date Helping Boards Oversee Management’s Risk Appetite

In Summary:

ERM implementations to date have not delivered promised benefits in a large percentage of organizations around the world; and failed in a spectacular way in dozens of the world’s largest and previously respected organizations.
Polling Question #2

What is the primary reason you think thousands of ERM initiatives have failed globally?

a) Not enough incentives for management to actively participate.
b) Boards of directors/senior management are OK with status quo.
c) Internal and external audit processes continue to focus on providing subjective opinions on “control effectiveness”, not quality assuring management reports on the current residual risk status/composite uncertainty related to important objectives.
d) ERM processes have fixated on analyzing individual risks, not providing useful information on the certainty/uncertainty of achieving key objectives linked to value creation/value erosion.
e) All of the above
f) Don’t know
SUPPLY-DRIVEN ASSURANCE
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #1: Fund IA / Complete audits on a small % of universe / Provide opinions on what constitutes “effective” control

A scene that repeats hundreds of thousands of times around the world:
The chairman of the audit committee extends the thanks of the board for the work done by Internal Audit in the previous year and asks two final questions that legal counsel has suggested he pose. He/she inquires:

"Are there any other concerns or control issues that I should be aware of?"

"Are controls adequate?"

The chief internal auditor responds:

"I have reported on the issues of significance noted in the year that I think you should be aware of. Management has, for the most part, been very cooperative and has indicated that they will take the steps they consider necessary to rectify the deficiencies noted during our audits. Although we have noted some problems in the course of our audits, overall, controls appear to be adequate in the areas we have reviewed."
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #2: Internal and external auditors form & report subjective opinions on whether they think controls are “effective” or “adequate”

Question: If the objective is “Prevent/minimize injuries/deaths in the home due to fire”, how many “controls” must be present to conclude controls are “effective” or “adequate”?

Should there be a tested escape plan? Should there be a fire extinguisher in the kitchen? In other rooms? Should there be two kinds of smoke detectors, battery and wired? Should there be a fire blanket in the kitchen? Should the house have a sprinkler system? Should parents have burn prevention/treatment training? Should there be an annual inspection by the local fire department or a fire risk specialist? Should there be an annual documented risk assessment that covers statistically probable risks? What about insurance coverage, contractual indemnities with suppliers, etc?

Answer: There is no such thing in real life as “effective controls”, only different levels of acceptable retained/residual risk. Auditors and regulators continue to pretend this isn’t a fundamental truth.
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #3: Senior management and boards don’t tell Internal Audit with any clarity what they want assurance on and how much

**Question:** How much should an organization spend on Internal Audit?

**Answer:** Without reasonable clarity on what senior management and the board want from internal audit, it is possible to propose and defend cost estimates ranging from $50,000 (tokenism) to a very high amount. All would allow the organization to report there is an Internal audit function that does audits, reports audit “findings,” and complies with the IIA IPPF standards.
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #4: Staff groups create & maintain a “Risk Register” / Assign “Risk Owners” / Create “risk heat maps” / Report top risks
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #5: Hire a Chief Compliance Officer and CRO but don’t communicate with clarity the company’s appetite/tolerance for violations, fines, jail sentences or scope of work.

**Questions:** Did the boards of Barclays/RBS/UBS know the bank was engaged in LIBOR manipulation? Should they have known?

Is the LIBOR scandal a failing of Internal Audit? Risk Management? Compliance? Bank boards? Or just a bad risk call by management that went badly wrong?
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #6: Annual reports now include a long list of “risks”. Regulators are increasingly concerned that these disclosures don’t always represent the important risks that boards should be focusing their attention on and investors should know about.

Following the 2008 global financial crisis regulators concluded public companies should report what they see as the biggest risks that could impact the company and describe how the board oversees risk. Most companies now do this in some form. Unfortunately it isn’t clear at this point, even to risk experts, if regulators want the biggest inherent/gross risks before considering “risk treatments”, or what the company considers the biggest retained/residual risk areas. The FRC in the UK has taken the lead in this area and indicated that a key test from their perspective is whether the board has specifically discussed and agreed the risks that will be disclosed in the annual accounts as the “principle risks and uncertainties” facing the company.

Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #7: Boards place heavy reliance on the company’s external auditors when their engagement letters severely limit scope and audit quality is variable.

In our opinion, the accompanying consolidated balance sheets and the related consolidated statements of operations, cash flows, changes in equity, and comprehensive income present fairly, in all material respects, the financial position of MF Global Holdings Ltd. and its subsidiaries (the “Company”) at March 31, 2011 and 2010, and the results of their operations and their cash flows for each of the three years in the period ended March 31, 2011 in conformity with accounting principles generally accepted in the United States of America. Also in our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of March 31, 2011, based on criteria established in Internal Control—Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

PRICEWATERHOUSECOOPERS LLP - New York, New York May 19, 2011

PROBLEM: Over 1.6 billion dollars of investor funds couldn’t be located shortly after this certification by PwC. This is not an isolated event nor is it meant to single out PwC. The current external audit paradigm has a fairly high error rate that isn’t likely to get better anytime soon in the absence of major changes in the auditing standards and methods used. Directors are increasingly expected to demonstrate that they have evaluated the effectiveness of the firm’s internal and external auditor – not a small task in a changing world.
Traditional “Supply Driven” Assurance: What’s wrong with the status quo?

Approach #8: Boards rely heavily on management, often using largely informal approaches without any form of independent assurance, to identify and report areas of high retained risk to the board – how well this happens varies widely.
Polling Question #3

3. In your opinion which of the following is the single biggest impediment boards face that truly want to oversee management’s risk appetite and tolerance?

a) Incentive systems that discourage management from providing a clear and candid picture to the board on the organization’s biggest retained risk positions.

b) Internal audit processes that were never designed to identify and communicate the biggest retained risk positions linked to key value creation and potential value erosion objectives.

c) ERM processes that don’t identify significant retained risk positions linked to key value creation and potential value erosion objectives.

d) Boards that don’t want to know about significant risks being accepted by management because of litigation/personal liability concerns.

e) All of the above

f) Don’t know
CHANGING YOUR APPROACH
Why change your IA/ERM approach?

• Intensifying regulatory pressure on boards post 2008 global crisis to visibly and actively oversee management’s risk appetite and tolerance

• Traditional IA/ERM methods weren’t designed for and don’t focus on identifying and communicating the state of residual/retained risk to boards

• Significantly heightened board risk oversight disclosure requirements that are likely to attract even more attention going forward

• Competitive differentiator/escalating client and investor expectations – especially from institutional investors and in high dependency customers/vendor situations

• Cost of capital - credit rating agencies now explicitly consider risk governance (e.g. see S&P expectations [http://bit.ly/jScZ9q](http://bit.ly/jScZ9q))
Why change your IA/ERM approach?

- Institutional investors are putting more focus and importance on risk oversight (e.g. ICGN expectations at [http://bit.ly/e7tSFu](http://bit.ly/e7tSFu))

- Increased senior management and board confidence key value creation objectives will be achieved and major value eroding events avoided or mitigate

- Current risk management/assurance approaches continue to allow major negative events/value erosion and all too often don’t work very well

- Strong regulatory push globally for public disclosure of “Risk appetite/risk framework statements” especially for financial institutions (e.g. see OSFI risk appetite statement expectations in Annex B [http://bit.ly/YG1vp1](http://bit.ly/YG1vp1))
Why change your IA/ERM approach?

- A lot of dissatisfied customers

BOARD-DRIVEN OBJECTIVE-CENTRIC IA & ERM
Board-Driven / Objective-Centric IA & ERM

- Clearly defined risk management and risk oversight accountabilities up to and including the board, who demand reliable information on significant retained/residual risk status linked to important value creation and potential value erosion objectives from management and assurance on reliability from IA.

- Board plays an active and visible role overseeing effectiveness of enterprise-wide risk management processes and management’s risk appetite/tolerance.

- CEO or his/her designate is responsible for providing the board a consolidated report on the state of residual risk including information on residual risk status currently rated as outside of corporate risk appetite/tolerance and residual risk acceptance decisions that have a high level of retained/residual risk, but have been rated by management as acceptable/within the company’s risk appetite/tolerance.
Board-Driven / Objective-Centric IA & ERM

- Internal “Risk Oversight Committee” selected by the CEO oversees implementation and maintenance of the company’s risk management framework, quality of the reports on residual risk status to the board, assigning objectives to “OWNER/SPONSORS”, and overseeing risk acceptance and risk rigour decisions made by OWNER/SPONSORS

- OWNER/SPONSORS must assign Residual Risk Ratings (“RRRs”) to objectives they are assigned and decide on the level/type of risk assessment rigour the objective(s) assigned warrant

- “Risk & Assurance Unit”/ “ERM Support Services” (which may be part of IA subject to caveats) has responsibility for creating and maintaining the risk assessment/risk status reporting processes
Board-Driven / Objective-Centric IA & ERM

• Internal Audit reports on reliability of risk management processes and the risk assessments completed, as well as objectives that it believes should be included in the OBJECTIVES REGISTER but were not, and where it believes higher/better risk assessment rigour than the risk assessment choice selected by OWNER/SPONSOR is warranted. (e.g. OWNER SPONSOR may have selected 2 minute rigor level and IA thinks it warrants 2 day rigor level)

• Internal audit uses the OBJECTIVES REGISTER as the core foundation for its work and annual work plans.

• An external specialist may be engaged periodically to report on reliability of the company’s risk management/risk oversight framework especially if IA plays a key role launching/maintaining risk management processes
Polling Question #4

4. In your opinion, which of the following is the #1 reason internal audit departments should champion demand driven/objective centric assurance?

a) Boards expect IA to help them meet emerging risk oversight expectations
b) IA is currently not seen as playing a key role helping organizations achieve key strategic objectives – this would help
c) It will refocus IA on the full range of possible “risk treatments” including risk share/transfer/finance not just “controls”
d) It will simply work better than status quo assurance approaches and better help organizations achieve key objectives and avoid disasters
e) If IA doesn’t provide the information boards need to meet new risk oversight responsibilities others will
f) All of the above
g) None of the above. IA should stick to providing subjective opinions on control effectiveness
Implementing BD/OC IA & ERM: Step-by-Step

• Drafting/approving Corporate Risk Policy
• Populating your “OBJECTIVES REGISTER”
• Assigning “OWNER/SPONSORS”
• Training OWNER/SPONSORS
• RiskStatusline™ assessment method
• Deciding on risk assessment rigor level
• Assigning “Residual Risk Ratings” (“RRRs”)
• Preparing consolidated entity-level risk reports
• IA assesses reliability of process and output
Implementing BD/OC IA & ERM
Corporate Risk Policy

Policy Overview

- PURPOSE
- SCOPE
- RISK MANAGEMENT PRINCIPLES
- CORPORATE RISK ASSESSMENT METHODOLOGY
- RISK MANAGEMENT ROLES AND RESPONSIBILITIES
  - Board of Directors/Audit Committee
  - CEO
  - Risk Oversight Committee
  - Heads of Departments
  - Compliance & Risk Department

(For a free sample Board-Driven policy contact tim.leech@riskoversight.ca)
Core Principles

1. Only objectives senior management and/or the board want formal assurance on should be included. Formal assurance costs money and this decision should be made consciously by key customers.

2. At minimum the entity’s top value creation objectives and objectives that could result in significant value erosion/reputation damage should be included.

3. Traditional internal audit universes and risk registers can be “reverse engineered” to identify the linked end result objectives. Often these have not included strategic objectives/top value creation objectives.
Core Principles

4. The top value creation objectives should be sourced from the organization’s strategic plans and budgets, executive compensation metrics (including the CEO’s), publicly disclosed objectives/strategies, and other available sources.

5. Top potential value erosion objectives can be identified via research – which events, other than flawed strategy/strategy execution, could lead to significant value erosion? This will category will include objectives linked to major legal violations, fraudulent financial statements, environmental incidents, major safety incidents, lawsuits for breach/negligence, cyber security, data loss/corruption, etc.
Implementing BD/OC IA & ERM
RiskStatusline™ Assessment Method

[Diagram of RiskStatusline™ assessment process]

- End Result Objective
  (Implicit or Explicit)

- Internal/External Context

  - External and Internal Environment
    the organisation seeks to achieve its objectives.

  - Threats to Achievement/Risks?
    Threats to Achievement/Risks are real or possible situations
    that create uncertainty regarding achievement of the objective.

- Risk Treatment Strategy
  Risk mitigators/controls
  risk transfer, share, finance
  (Selected consciously or unconsciously)

- Residual Risk Status
  Residual Risk Status is a composite snapshot
  that helps decision makers assess the
  acceptability of the retained risk position.

  Status data includes performance data,
  potential impact(s) of not achieving the
  objective, impediments, and any concerns
  regarding risk treatments in place. (NOTE:
  “control deficiencies” are called concerns)

- Acceptable?
  Is the residual risk status acceptable to the
  work units? Management? The Board? Other key stakeholders?
  (i.e. managed within risk appetite/tolerance)

  - NO
    Re-examine risk treatment strategy
    and/or objective and develop action plan

  - YES
    Risk Treatment Optimized?
      Is this the lowest cost combination of
      risk treatments given our risk appetite/tolerance?

      - NO
        YES – Move On

      - YES
        Risk Treatment Optimized?
Implementing BD/OC IA & ERM
Assigning RRRs

**Risk Statusline™**

- End Result Objectives (Implicit or Explicit)
- Internal/External Context
- Threats to Achievement/Risks?
- Risk Treatment Strategy
  - Risk mitigators/controls
  - Risk transfer, share, finance (Selected consciously or unconsciously)
- Residual Risk Status
  - Acceptable?
    - NO: Re-examine risk treatment strategy and/or objective and develop action plan
    - YES: Risk Treatment Optimized?
      - NO: Move to next level
      - YES: Move On

### Residual Risk Rating Definitions

0. Fully Acceptable - Residual risk status is acceptable. No changes to risk treatment strategy are required.

1. Low - Inaction on unacceptable terms could result in very minor negative impacts. Ad hoc attention may be required to adjust status to an acceptable level.

2. Minor - Inaction or unacceptable terms could result in minor negative impacts. Routine management attention may be required to adjust status to an acceptable level.

3. Moderate - Inaction on unacceptable risk status could result in or allow continuation of mid-level negative impacts. Moderate senior management effort required to adjust status to an acceptable level.

4. Advanced - Inaction or unacceptable risk status could allow continuation of or exposure to serious negative impacts. Senior management attention required to adjust risk status.

5. Significant - Inaction on unacceptable risk status could result in or allow continuation of very serious negative impacts. Attention required to adjust status to an acceptable level.

6. Major - Inaction on unacceptable risk status could result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.

7. Critical - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very major entity level negative consequences. Analysis and corrective action required immediately.

8. Severe - Inaction on unacceptable risk status virtually certain to result in or allow continuation of very severe negative impacts. Senior board level attention urgently required.

9. Catastrophic - Inaction on unacceptable risk status could result in or allow the continuation of catastrophic proportion impacts. Senior board level attention urgently required to avert a catastrophic negative impact on the organization.

10. Terminal - The current risk status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from the board and senior management to prevent the demise of the entity.
Implementing BD/OC IA & ERM  
Assigning RRRs

• When a decision is made to include an objective in the “OBJECTIVES REGISTER” the “OWNER/SPONSOR” must assign a “RESIDUAL RISK RATING (“RRR”)” to the objective and decide on the level of risk assessment rigour from very low rigour (takes minutes) to very high rigour (takes days)

• Definitions of RRR ratings are on the prior slide. RRRs must be revisited periodically and adjusted by the OWNER/SPONSOR as formal risk assessments are done and/or new information emerges
## Implementing BD/OC IA & ERM

### Deciding on Risk Assessment Rigour

<table>
<thead>
<tr>
<th>Risk Status Analysis Level</th>
<th>Overview of Assessment Options</th>
</tr>
</thead>
</table>
| **Quick Start**           | • Define/refine end result business objectives and “Owner/Sponsors”  
                          | • Assign an initial Residual Risk Status rating for each objective from 0 (fully acceptable) to 10 (entity catastrophic). The rating is linked to the level of management/board attention. |
| **Importance Prioritization Option** | • Quick Start requirements (see above)  
                          | • Assign an objective importance rating – importance to the unit  
                          | • Assign an objective importance rating – importance to the entire corporation  
                          | • Document current level of risk status knowledge and target level. The higher the gap between current and target the higher the objective’s priority. |
| **High Level Risk Assessment** | • Quick Start and Importance Prioritization options (see above)  
                          | • Document threats to achievement/risks, likelihood and consequences of risks, and risk level  
                          | • Document “best guess” current mitigation estimate for each threat/risk and traffic light rating  
                          | • Develop and assign responsibility for risk treatment action items for risks with unacceptable residual risk ratings |
| **Full RiskStatusTM Assessment** | All steps above plus:  
                          | • Document key risk treatments in place to manage significant risks  
                          | • Document current performance information for the objective using best available information (“KPI” information)  
                          | • Document impact information for the objective including what would be the consequences to company, unit, individuals, community etc if the objective wasn’t achieved in whole or part. (NOTE: This is impact of non-achievement of objective not individual risks impacts)  
                          | • Document known concerns – risk treatments/controls known to be missing, deficient or needing improvement  
                          | • Document any impediments – elements outside of the control/resources of the business objective owner that would prevent them from adjusting retained risk level  
                          | • Assign action items |
Very simply, consolidated residual risk reports provide details on important value creation and potential value erosion objectives that have high residual risk ratings (see prior slides). High RRRs indicate increasingly material unacceptable retained risk positions with potential to have a significant negative impact on the achievement of specified end result objectives.
Business Case for BD/OC IA & ERM

1. Primary responsibility for risk management, risk assessment, and risk reporting is positioned squarely with management.
2. Boards are provided with more reliable, quality assured entity level information on the current state of residual/retained risk. This helps boards understand and oversee management’s risk appetite and tolerance.
3. The approach focuses attention on the upside of risk management by emphasizing the need to include the organization’s top value creation objectives in the OBJECTIVES REGISTER. OWNER/SPONSORS of those objectives are incentivized to use risk assessment tools to increase certainty/reduce uncertainty that top value creation objectives will be achieved while still operating within a tolerable level of retained/residual risk.
4. Allows an organization to make conscious, visible, well thought-out decisions on which business objectives warrant the cost of formal assurance/risk management and how much assurance is required.


6. Encourages users to consider not only the acceptability of the residual/retained risk status, but also whether the current “risk treatments in place are optimized – i.e. the lowest possible cost combination that would still produce an acceptable level of residual risk.

7. Links performance information on specific objectives to related risks and risk treatments allowing users to see the impact of any changes made to the risk treatment design.
8. Internal audit departments are provided with clear requirements from senior management and/or the board detailing which objectives they want formal assurance on and how much. This helps estimate what internal audit’s annual budget should be. IA’s main role is to provide assurance/opinions on the reliability of the entity’s risk assessment processes, and the consolidated report on residual risk status for the board of directors.

9. ERM support teams are provided with clear deliverables that detail which objectives senior management and/or the board want risk status information and the level of target level of risk assessment rigor. The onus is on OWNER/SPONSORS to request training/facilitation/assessment assistance from the ERM support team to support risk assessment rigor decisions. OWNER/SPONSORS, the Risk Oversight Committee, and/or the board have decided is warranted.
BPS Resolver and Risk Oversight Inc. have partnered to bring “Next Generation” risk and assurance software to market.

NAME OF THE SOFTWARE: RiskStatusNet™
UNDERLYING METHODOLOGY: RiskStatusOversight™ (BD/OC)
BETA TESTING LAUNCH DATE: April 1, 2013
To learn more and/or sign-up to be among the first to see this exciting new approach to ERM and Internal Audit contact:
peter.trinz@bpsresolver.com
Polling Question #5

In your opinion, which of the following is the most persuasive benefit of the board driven/objective centric approach?

- a) Accountability is more closely aligned and assigned to those with responsibility for deciding on what constitutes an acceptable retained risk position.
- b) The method forces boards, senior management, ERM support staff and IA to focus on the really important value creation objectives and objectives with high value erosion potential.
- c) It will cause IA to focus on important value creation objectives and the full range of possible “risk treatments” to address risks not just “controls”
- d) It should work better than status quo assurance approaches and better help organizations achieve key objectives and avoid disasters
- e) All of the above
- f) Don’t know
Questions???

Tim Leech

tim.leech@riskoversight.ca

www.riskoversight.ca

Twitter: www.twitter.com/riskoversight